(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 158 386 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
28.11.2001 Bulletin 2001/48

(51) Int Cl.[7]: **G06F 1/00**

(21) Application number: **01100910.7**

(22) Date of filing: **16.01.2001**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **24.05.2000 JP 2000157954**

(71) Applicant: **Hitachi, Ltd.**
Chiyoda-ku, Tokyo 101-8010 (JP)

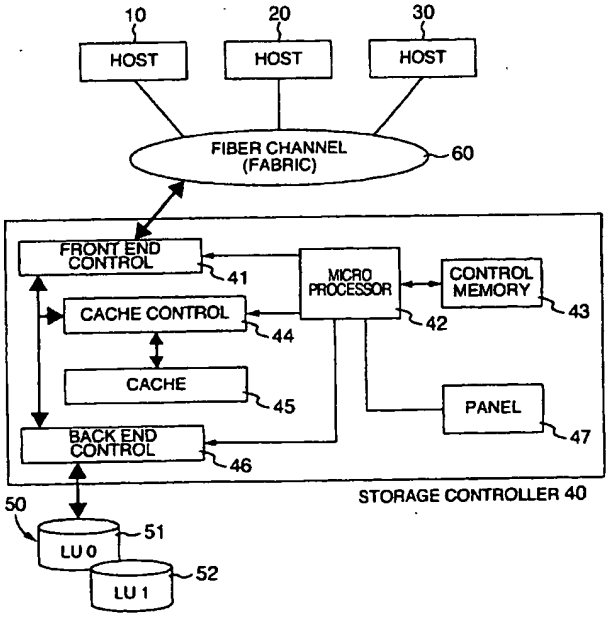
(72) Inventors:
- **Kamano, Toshimitsu, Hitachi, Ltd., Intell.Prop.Grp**
  Chiyoda-ku, Tokyo 100-8220 (JP)
- **Takamoto, Kenichi, Hitachi, Ltd., Intell.Prop.Grp.**
  Chiyoda-ku, Tokyo 100-8220 (JP)

(74) Representative: **Strehl Schübel-Hopf & Partner**
Maximilianstrasse 54
80538 München (DE)

(54) Method and apparatus for controlling access to storage device

(57) The storage regions (50) under command of a storage controller (40) can be simply enabled and disabled to access to by automatically registering connected host computers (10, 20, 30). Such system can be achieved by taking a step (503) of acquiring N_Port_Name information included in a login frame (70) from the host computers, and a step (507) of displaying a table (200, 201, 202; 700) of access right of host computers (10, 20, 30) to a logical unit (51, 52) under command of storage controller. A security table (202, 202; 700) for the storage controller (40) can be generated by supervisor's setting the access enable/disable flag information (508).

FIG.1



EP 1 158 386 A2

Description

BACKGROUND OF THE INVENTION

[0001] The present invention generally relates to security setting for prevention of illegal access between information processors. Particularly, the invention relates to a storage system for prevention of illegal access when a request occurs to access to a storage region under command of a storage controller in a computer system having a network provided between a high-rank unit (host computer) and the storage controller (storage system), and relates to the computer system including this storage system.

[0002] In the fiber channel protocol standardized by ANSI, X3T11, a great number of apparatus can be connected, and a large variety of protocols such as SCSI, ESCON and TCP/IP can be simultaneously operated. However, when it is feared that data in storage devices is destroyed by an access which a different file system makes due to a different kind of protocol, it is necessary to take a security measure against that.

[0003] To assure this security, as described in JP-A-10-333839, a table showing information for uniquely identifying host computers and to either permit or reject access to storage regions under command of a storage controller is provided within the storage controller. At the time of access, by referring to this table, it is possible to reject the access from the other apparatus than the host computers that are permitted to access, and hence prevent illegal access.

[0004] This identifycation information is an array of 48-bit digits called N_Port_Name, unique to each host bus adapter. Under the condition that the identification information for host computers are previously registered within the storage controller, the host computers can make access to storage regions within a storage device under command of the storage controller.

[0005] In order to previously register the host computer identifying information within the storage controller, the user or supervisor is first required to examine the N_Port_Name expressed by 48-bit digits that has an eight-byte region peculiar to a host computer by use of a manager connected to host computers through LAN. Then, it is necessary that this number be noted and registered in the storage controller by his own hand. Therefore, it is feared that if a wrong N_Port_Name is registered by mistake as the correct one of a host computer, this host computer cannot access to a storage region or an undesired host computer might make access to a storage region and destroy data.

[0006] Moreover, when information of either permitting or rejecting access to a large number of host computers is registered, it takes much time. Therefore, it is desired that this identification information be simply acquired and set.

SUMMARY OF THE INVENTION

[0007] Accordingly, it is an object of the invention to provide a system capable of acquiring information that uniquely identifies the connected host computers and automatically registering it within a storage controller, thereby making it possible simply to either permit or reject access to storage regions under command of the storage controller.

[0008] To achieve the above object, according to the invention, the host-identifying information is first acquired from a frame transmitted from the corresponding host computer, and registered in the storage controller, and then flag information is set to change for permitting that host computer to access by the supervisor's operation.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009]

Fig. 1 is a block diagram showing a hardware structure of an embodiment of the invention.
Fig. 2 is a diagram showing the format of a frame.
Fig. 3 is a diagram showing the details of the frame header.
Fig. 4 is a diagram showing the sequence of log-in between host computer and device.
Fig. 5 is a flowchart for log-in, and security table registration and setting.
Fig. 6 is a flowchart for addition of a host computer to an operating computer system.
Figs. 7A, 7B, 7C and 7D show examples of the security table.
Fig. 8 is a diagram showing an example of the display panel used at the time of registering security information.
Fig. 9 is a flowchart for the process to INQUIRY command.
Fig. 10 is a flowchart for the process having a security table auto-setting mode.
Fig. 11 is a flowchart for the process taken when a device intermits.
Fig. 12 is a flowchart for security table change and re-login.
Fig. 13 is a diagram showing a computer system having SAN manager.

DESCRIPTION OF THE EMBODIMENTS

[0010] Embodiments of the invention will be described with reference to the accompanying drawings.

[0011] A description will be made of a computer system constructed by use of a storage controller and magnetic disk units as a storage system according to the present invention, and a network constructed by providing a fiber channel between the storage system and host computers, or a computer system under the so-called

SAN (Storage Area Network) environment.

[0012] The fiber channel is a protocol having a serial transfer system with no own command set. Since it sends information asynchronously, the frequency bands of transmission media can be effectively used.

In addition, instead of having no own commands, a physical transfer system is used as a carrying way for a command set such as SCSI or ESCON, thereby making it possible to faster transfer data of various kinds while the background art resources are being inherited.

[0013] Fig. 1 is a block diagram showing a hardware structure of a computer system according to the invention. Referring to Fig. 1, there are shown host computers 10, 20, 30, each acting as a central processing unit for performing data processing. A plurality of magnetic disk drives 50 are storage units with storage media that are connected in an array under command of a storage controller 40. The storage controller 40 is a disk array system for controlling these magnetic disk drives 50.

[0014] The storage controller 40 is constructed by a front end control unit (channel adapter) 41 for controlling the fiber channel protocol to the host computers 10, 20, 30, a microprocessor 42 for controlling all the storage controller 40, a nonvolatile control memory 43 for storing a microprogram for controlling the operation of storage controller 40, data for control and each table described later, cache 45 for temporarily storing (buffering) data, a cache control unit 44 for controlling this cache 45 to read and write data, a back end control unit (disk adapter) 46 for controlling a protocol used to the magnetic disk drives 50 to control data transfer to or from the magnetic disk drives 50, and a panel 47 on which information is set.

[0015] The magnetic disk drives 50 are expressed as logically divided regions. In the SCSI protocol, these regions are called LU (Logical Unit), and numbered by LUN (Logical Unit Number). In this embodiment, two regions of LU0 (51) and LU1 (52) are shown as LU of LU0 and LU of LU1.

[0016] The host computers 10, 20, 30 and the storage controller 40 are connected through a fiber channel 60 as an interface i.e., via a switch called "Fabric".

[0017] The operation of the system shown in Fig. 1 will be described. As an example of this operation, it is assumed that data is transferred between the host computer 10 and the LU0 (51) provided within the disk drive 50 through the storage controller 40. The host computer 10 logins the storage controller 40. Then, when the host computer 10 issues an access request (I/O request) to the LUO (51), the front end control unit 41 that received this request sends an interruption request to the microprocessor 42. The microprocessor 42 controls the control memory 43 to store command information from the host computer 10 and information for identifying the host computer 10. When the host computer 10 is previously permitted to access to the LU0 (51), the microprocessor 42 confirms the command type.

[0018] When the confirmed command is Read command, the microprocessor 42 decides if the data block to be accessed exists in the cache 45. If this data exists, it is transferred to the host computer 10, and the end sign is sent to the host computer 10. If the data is not present, the back end controller 46 is operated to read the data block from the LU0 (51), and the cache control unit 44 controls the read data to be stored in the cache 45. Then, the microprocessor 42 orders the front end control unit 41 to transfer the data stored in the cache 45 to the host computer 10, and to report the end sign to the host computer 10.

[0019] If the confirmed command is Write command, the microprocessor 42 controls the cache 45 to store the data to be written, and sends the end sign to the host computer 10. Then, the cache control unit 44 is used to send this data to the LU0 (51) and completely write therein.

[0020] The basic unit of data that the fiber channel handles is called frame. This frame will be described with reference to Fig. 2. As shown in Fig. 2, a frame 70 is formed of a start-of-frame (SOF) 71, a frame header 72 of 24 bytes for link operation control and for characterizing the frame, a data field 73 of data itself to be actually transferred, a cyclic redundancy check (CRC) 74 of 4 bytes, and an end-of-frame (EOF) 75. The data field 73 is variable in the range from 0 to 2112 bytes.

[0021] The SOF 71 is an identifier of 4 bytes placed at the head of the frame. The EOF 75 is an identifier of 4 bytes placed at the back of the frame. The SOF 71 and the EOF 75 define the frame. A signal of idle flows in the fiber channel when there is no frame.

Fig. 3 shows the format 80 of the frame header 72.

[0022] The format of the frame header 72 will be described below with reference to Fig. 3. The frame header 72 is formed of six words of 32 bits each. A destination identifier D_ID (Destination ID) 81 of 23rd - 0th bit of word 0 is an address identifier for the frame receiving side. A source identifier S_ID 82 of 23rd - 0th bit of word 1 is an address identifier of three bytes for identifying a port of the transmission source of the frame. This identifier has a meaningful value in all frames transmitted and received. The S_ID 82 is the information capable of dynamically and uniquely identifying a host computer, and is a value reported from the host computer at the time of PLOGI (described later). However, this S_ID 82 is, for example, a value dynamically changing each time the system is started, and assigned at the time of initialization by Fabric in FC-PH (Fiber Channel Physical and Signaling Interface: US standard of fiber channel). The value to be assigned deponds on N_Port_Name and Node_Name which each port has.

[0023] The kind of frame is roughly divided into data frame and link control frame on the basis of the function. The data frame is used for information transfer, and has data and commands provided at the payload section of the data field for use in a high-rank protocol. The link control frame is generally used for indicating if the frame transmission has been successfully or unsuccessfully

made. As an example of the link control frame, there is a frame for indicating that a single frame has received or a frame for notifying parameters of transfer at the time of log-in.

[0024] In the fiber channel interface, a host computer sends to a device a frame of port log-in PLOGI (N_Port Login) command including a communication parameter, and the device accepts this frame, thus communications being made possible. This is called login.

[0025] A description will be made of the format of PLOGI frame that is a communication request of a certain host computer to the storage controller 40. In the data field 73, the first 8-bytes region of the twentieth to twenty-seventh byte (fifth to sixth word) is a region for storing the N_Port_Name, and the second 8-bytes region of the twenty-eighth to thirty-fifth byte (seventh to eighth word) is a region for storing the Node_Name.

[0026] The device sends to the host computer a frame called ACC (Accept) at the time of accepting the request, or LS_RJT (Link Service Reject) at the time of rejecting the request.

[0027] Fig. 4 shows a login sequence 100. The host computer as a source of login request sends the PLOGI frame to the storage controller 40 of a device as a destination of login request. This PLOGI frame has its frame header 72 including S_ID 82 and other information, and its data field 73 including the N_Port_Name and Node_Name of the login request source.

[0028] The storage controller 40 takes information out of this PLOGI. When accepting the login, it transmits ACC frame to the source of login request. When rejecting the login, the storage controller 40 transmits to the host computer a frame called LS_RJT against the PLOGI frame.

[0029] The security information acquisition and automatic registration according to the invention will be described with reference to Fig. 5. Here, in place of N-Port_Name, WWN (World Wide Name) that is similarly expressed by an array of 48-bit digits is used as transmission source identifying information. The WWN has a value of 8 bytes peculiar to each apparatus as does the N_Port_Name. It may include Port_Name peculiar for each port and Node_Name peculiar to each node.

[0030] After a peripheral unit such as storage controller 40 is first started, the host computer 10, 20, 30 is started up (step 501). Each host computer issues a PLOGI frame as a login request frame including N_Port_Name information peculiar to each host.

[0031] The microprocessor 42 of the storage controller 40 receives the frame sent through the port (not shown) of the front end control unit 41 (step 502). Then, the microprocessor 42 cuts off the WWN information out of the frame, forces the buffer (not shown) of the cache 45 to store that information, and refers to a port security table (host computer information table) 200 defined within the control memory to see if it is already registered in the WWN list of the table 200 (step 503). The frame at the time of actual I/O request (Inquiry) which will be described later has no N_Port_Name added, but only S_ID added the value of which changes for each time of starting. Thus, the microprocessor 42 cuts off S_ID out of the frame header of PLOGI, and WWN out of the data field, and generates the security table (host computer information table) 200, as shown in Fig. 7A, to enable N_Port_Name to be pulled out of S_ID at the time of Inquiry. This table is stored in the control memory 43. It is assumed that the part of list in which the WWN information of port security table 200 is stored has initially a value irrespective of the WWN information as a default. Each time each of the host computers issues PLOGI frame, the WWN (or N_Port_Name) and S_ID included in the PLOGI frame are automatically registered in the security table 200.

[0032] If it is decided to be false (YES at step 503'), the cut-off WWN information of host bus adapters 11, 21, 31 of host computers 10, 20, 30, assumed as host A, host B and host C, are stored in the security table 200 successively (step 504). Since the WWN information inserted within the frame the host computer 10, 20, 30 has issued does not agree with the values registered as default within the table 200, the microprocessor 42 of the storage controller 40 sends LS_RJT frame having a reject parameter for rejection against the connection back to the host computer 10, 20, 30 (step 505).

[0033] Since the storage controller 40 cannot accept the I/O of host computer 10, 20, 30 at the time of newly starting as describe above, the panel 47 is used to assign those host computers to the respective ports of the front end control unit 41 that the storage controller 40 can permit to access to the ports. The supervisor uses the panel 47, and orders it to perform a port security change task for port in order that the host computer 10 can access to the controller via a port of front end control unit 41. When a port security change window is brought about by pushing keys of a key area 472 of panel 47, WWN information is displayed in the order of automatic registration on the WWN column of table 200.

[0034] As shown in Fig. 8, the automatically registered Host A, host B and host C are displayed on the panel screen. The supervisor operates keys to select the Host A as WWN information of host bus adapter 11 of host computer 10, and to select the Enable of the port access permit/reject pair flag information on the table, thus enabling the host to access. This port access permit/reject flag information is previously set to be Disable as default. Similarly, the access from host computers 20 and 30 can be enabled (steps 506, 507, 508, 514). An example of how to enter is shown in Fig. 8. The panel 47 is shown in Fig. 8. In the panel 47, a display 471 is shown to indicate the automatically registered host computers (in this case, Host A and Host B are already registered, and Host C is to be newly registered). When Host C is selected by pushing the arrow keys of the key set 472, the LU access permit/reject flag information can be set to be Enable or Disable. Then here the supervisor selects Enable thus enabling this host to

access. It is better to set Disable as the default of this LU access permit/reject flag information. The key set 472 may have keys for numerals that allow WWN to be manually inputted by hand as in the background art. In Fig. 8, for the sake of simplicity, a single LU (storage region) is shown.

[0035] Next, the host computers 10, 20, 30 make re-recognition processing for the connected devices (step 514).

[0036] The host computer 10, 20, 30 again issues PLOGI frame as a login request frame, and the microprocessor 42 of storage controller 40 receives the frame fed through a port of front end control unit 41 (step 502). Then, the microprocessor 42 cuts off the WWN information out of the frame, and compares it with the WWN information list within the port security table 200 (steps 503, 503'). When it is decided to agree because it is already registered (NO of step 503'), the microprocessor sends back to the host computer 10, 20, 30 a frame indicating that login is possible. Thereafter, login processing is continued, and the storage regions 51, 52 under command of storage controller 40 can be accessed by the host computers 10, 20, 30 (steps 515 to 517).

[0037] At step 503', when it is recognized that a new host computer is connected, that the new host computer has been corrected is indicated on the panel display. At this time, the supervisor is urged to make mode selection for the registration in the security table. The modes that can be selected at step 506 include a mode in which WWN itself is used to register, and a mode in which Company_ID included in WWN is used to register. The fact that a new host computer has been connected may be indicated by means of blinking on the display, guide using voice or other ways that the supervisor can perceive.

[0038] The Company_ID will be described. The N_Port_Name of 8 bytes includes Company_ID (selected when a four-bit area of 60th bit to 63rd bit has a particular value) in a 24-bit area of 36th bit to 59th bit, and VS_ID (Vendor Specific Identifier) in a 36-bit area of 0th bit to 35th bit. Here, a unique value is allocated to the Company_ID of each vendor. That is, the same vendor has the same value.

[0039] Under the security for preventing data damage by I/O from a host computer having a different protocol and different file system, the same device can be often accessed by host computers of the same vendor. Therefore, there will be often no trouble even if security is set up for each vendor. Thus, since the access enable/disable conditions can be provided for a unit of a plurality of host computers, the security table (access enable/disable table) can be more easily generated.

[0040] When the supervisor selects the registration of WWN (of each of a plurality of host computers to be registered), and when any security table is not generated yet, e.g., when the system is started, the microprocessor 42 recognizes LU that is a storage region under command of storage controller 40. Then, it generates a security table (access enable/disable table) 201 of host computes and LU as shown in Fig. 7B. If the security table 201 is previously generated, e.g., when a host computer is added or restarting is made, a host computer corresponding to a new WWN is added to the security table 201, thus a new security table being generated.

[0041] This security table 201 is shown in the display of panel 47 (step 507). The supervisor inputs only access enable or disable designation for the host computers on the table by use of the panel 47 (step 508).

[0042] When the supervisor selects the registration of each vendor, the microprocessor 42 cuts Company_ID off out of WWN (step 509). Then, an access enable/disable table 202 of vendor and LU as shown in Fig. 7C is generated and displayed as at step 507 by use of this Company_ID (step 510). The supervisor enters only the access enable or disable designation for the host computers on the table by use of panel 47 (step 511).

[0043] Since the security table 201 shows the relation between the host (WWN) and LU, the access enable and disable designation for the host computers (WWN) each having a Company_ID are automatically entered with reference to the access enable/disable table 202 generated at step 511, thus replacing the process at step 507 (step 512).

[0044] Thus, the security table 201 is completely set up by the above input operation and updated (step 513).

[0045] After updating the security table 201, the microprocessor 42 issues GPN_ID (Get_Port_Name) to host computers, causing the host computers to issue PLOGI (step 514).

[0046] Since a new WWN is not handled this time, NO is selected at step 503', and the process goes to step 515.

[0047] When WWN is known at step 503', login continues, and it is decided if this WWN can login in storage controller 40. For this purpose, with reference to security table 201 it is decided if this WWN has right to access to a given LU (LU0 or LU1 in Fig. 1) under command of storage controller 40 (step 515).

[0048] ACC is sent back to the host computer in which the access right is already set (step 516), and login operation is completed (step 517).

[0049] LS_RJT is transmitted back to the host computer that has no access right (step 518), and login is rejected (step 519).

[0050] When a plurality of host computers are newly connected, e.g., when the system is initially started, the supervisor cannot recognize which host computer corresponds to a WWN. Therefore, at step 506, when registration is made for each WWN, the relation between host and WWN is checked from the SAN manager separately connected to the system. Under this checking, the supervisor can generate the security table 201 by only entering the presence or absence of the access right.

[0051] The SAN manager will be described with reference to Fig. 13. The host computers 10, 20, 30 and

the storage controller 40 are also connected through a local area network (LAN) 61 other than the fiber channel Fabric 60. SAN manager unit 90 and the fiber channel Fabric 60 are also connected to this LAN 61. The SAN manager unit 90 is PC or WS, and acquires information about SAN system construction from the host computers 10, 20, 30, storage controller 40 and fiber channel Fabric 60 via LAN 61.

[0052] In addition, at step 506, for the case in which vendor registration mode is selected, the control memory previously stores the Company_ID of each vendor, and thus it can be known that a new WWN corresponds to a particular host computer of a certain vendor. Therefore, even at the time of initial setting, by only mode selection it is possible that the supervisor generates the security table 201 without entering the presence or absence of access right.

[0053] A description will be made of the case where a new host computer is added to the operating computer system with reference to Figs. 1 and 6. In the system construction shown in Fig. 1, it is assumed that the host computer 30 is added under the operation of the system that has no host computer 30. When the host computer 30 is newly connected to the system, i.e., when the cable connected to the host bus adapter (not shown) of host computer 30 is connected to the switch 60 of the fiber channel Fabric, fabric login FLOGI is executed between the host computer 30 and the switch. The fiber channel Fabric switch 60 sends to all connected devices, RSCN (Registered State Change Notification) that indicates change of state (step 601). The microprocessor 42 of the storage controller 40 that has received this notification transmits an ACC (Accept) frame (step 602).

[0054] Since the added host computer does not correspond to any one of the host computers under login, Get Port Name (GPN_ID) is transmitted to the host computer 30 to request N_Port_Name information (step 603). Since the received N_Port_Name information is of course not registered even referring to the N_Port_Name information list of security table 200, the N_Port_Name information of the added host computer 30 is stored in the port security table 200 (step 604).

[0055] Since the S_ID of the host computer 30 is not acquired yet, the storage controller 40 cannot accept the access by the host computer 30 under this condition. Therefore, the supervisor assigns the host computer, and makes it be enabled to access by use of panel 47. The supervisor requires to execute a port security change task for port P0 on the panel 47 in order that the host computer 30 can be enabled to access via port P0 of front end control unit 41. As a result, the N_Port_Name information is displayed on the security table 200 at the N_Port_Name item column.

[0056] When Host C is selected as the automatically registered N_Port_Name information of the host bus adapter 31 of host computer 30 in response to GPN_ID, the port access permit/reject pair flag information can be changed on the table. The supervisor selects Enable, thus this host being enabled to access (step 605). Here, the host computer 30 can make re-recognition processing for the connected device (step 606). Then, login process is performed so that the S_ID corresponding to the host computer 30 can be acquired from the host computer 30. The storage regions 51, 52 under command of storage controller 40 can be accessed by the host computer 30. After the subsequent reception of PLOGI frame, the process of entering all items concerning the host computer 30 on the security table 200 ends.

[0057] While N_Port_Name information is used for the description with reference to Fig. 6, WWN information may be used therefor.

[0058] In addition, while the security table (host information table) 200 and security table (access enable/disable table) 201 or 202 are shown as separate tables in Figs. 7A through 7C, they are managed as one table as shown in Fig. 7D.

[0059] The execution of Inquiry command will be described with reference to Fig. 9. The Inquiry command is a command to inquire, before the start of I/O process, the installation of the logic devices associated with the process. Specifically, this command is a request to inquiry information before the host computer issues a request to access to the storage region LU under command of storage controller 40. This command is a standard command that is surely supported in SCSI.

[0060] The detailed format of frame header 72 will be described. The host computer to access to LU sends a frame including Inquiry command to the storage controller 40 having the LU to be accessed (step 901). This frame includes the S_ID 82 of the host and LUN as an LU identifier for inquiry assigned in PLOGI.

[0061] To issue Inquiry and execute I/O, the S_ID 82 is cut off out of the Inquiry frame (step 902). Then, the N_Port_Name corresponding to the S_ID 82 is acquired from the security table 200 showing the relation between N_Port_Name (or WWN) and S_ID 82. Thus, it is decided which host computer has issued Inquiry (step 903).

[0062] In addition, from the security table 201 it is decided if the decided host computer has right to access to the LU for I/O (step 904). If it has right, ACC is sent back to the host computer that has issued Inquiry for access (step 905). Then, I/O process is performed (step 906). If it has no right, LS_RJT is transmitted back to the host computer (step 907), rejecting I/O request (step 908).

[0063] Thus, I/O process is accepted or rejected, and Inquiry ends (step 909).

[0064] With reference to Fig. 10, a description will be made of another embodiment having the function for the mode in which security setting is automatically registered in addition to the registration of host computers.

[0065] Steps 1001 through 1009 are the same as steps 501 through 509 given in Fig. 5, and thus will not be described.

[0066] After clipping Company_ID at step 1009, the user decides to select manual or automatic security reg-

istration (step 1010).

[0067] If manual registration is selected, steps 1011 and 1012 are executed. These steps are the same as steps 510 and 511 shown in Fig. 5, and thus will not be described.

[0068] If automatic registration is selected, the microprocessor 42 checks if the host computers registered on the security table 200 include the same one as Company_ID of new WWN (step 1013).

[0069] If there is not, the automatic setting of security cannot be made, and thus the process goes to step 1011 as in the manual setting. If there is the same Company_ID, the security setting of that Company_ID is copied as a Company_ID of new WWN, thus the access enable/disable setting input for that host being omitted (step 1014).

[0070] Step 1015 and the following steps after generating security table for each vendor are the same as step 515 and the following steps shown in Fig. 5, and thus will not be described.

[0071] Description will be made of the case where a host computer is temporarily stopped or a host bus adapter is replaced due to failure in the operating computer system, with reference to Fig. 11.

[0072] When a certain host computer is extracted from the system (step 1101), or when the cable connected to the host computer is disconnected from the switch of Fabric 60, the switch (not shown) of fiber channel 60 sends RSCN indicating change of state to all connected devices (step 1102). The storage controller 40 that has received this notification sends accept (ACC) frame (step 1103). The storage controller 40 confirms if the host computer informed of by the received RSCN exists in the host computers now under login (step 1104). If there is, GPN_ID is sent to that host computer (step 1105).

[0073] The host computer extracted from the system is disconnected, and thus cannot respond to GPN_ID. Therefore, the storage controller 40 cannot receive accept (FS_ACC) (step 1106). Thus, the storage controller 40 internally executes logout process for this host computer. Then, it changes the access enable/disable flag information of security table 201 to Disable, or makes that host be disabled to access (step 1107). When the host is again connected after replacing the host bus adapter, N_Port_Name information is changed, and thus the same mode as the new provision/addition of a host is brought about.

[0074] Here, at step 1107 it is possible to set not to change the access enable/disable flag information of security table 201. Then, if the host computer is temporarily stopped or resumes its operation after having been completely repaired, it can access to the same storage region as before the stop without again setting security table 201. The host bus adapter replacement process involves the connection and disconnection of the cable of the same port. Thus, under the mode of "deciding host adapter replacement due to failure", automatic access setting can be made without enabling access on panel 47 by supervisor. On the contrary, under the mode of "access enable/disable", addition process is executed as in the embodiment for host addition.

[0075] LU security change will be described with reference to Fig. 12. The security table 201 or 202 is started to change by use of panel 47 shown in Fig. 8 (step 1201). First, change for each WWN or each vendor is selected as a change mode (step 1202).

[0076] When change for each WWN is selected, the microprocessor 42 controls panel 47 to indicate a list of host computers on the display 471 (step 1203). Then, the supervisor operates the key buttons 472 to change the access enable/disable conditions of host to be changed (step 1204).

[0077] When change for each vendor is selected, the microprocessor 42 cuts Company_ID away from WWN of host information table 200, and generates the security table (access enable/disable table) 202 showing the access enable/disable conditions of vendors (step 1205). Then, the vendor-access security table 202 is indicated on the display 471 of panel 47 (step 1206). The supervisor operates the key buttons 472 to change the access enable/disable conditions of a vendor to be changed (step 1207). The microprocessor 42, on the basis of the results, searches for the WWN having the Company_ID of the vendor changed, and makes the access enable/disable table have the same contents as at step 1204 (step 1208).

[0078] Then, the microprocessor 42 changes the security table 201 (step 1209). Moreover, it issues a command for re-recognition to the host computer (step 1210). The host computer sends PLOGI in response to this command, leading to login (step 1211). In order to make the access enabled host be disabled, it is necessary that the host computer to be disabled to access be internally made logout by the storage controller 40 before the re-recognition process.

[0079] While in the above three examples, the access enable/disable operations are made for each LU unit of front end control unit 41 of storage controller 40, it is possible to make setting not for each LU but for each storage controller 40. In that case, the accessed ones of the security table 201 are not LU but storage controller 40. Moreover, when the front end control unit 41 has a plurality of ports, the access right of host is set for each port, thereby making it possible to avoid competition among host computers or provide priority to the host computers.

[0080] In addition the security system can also be constructed by transferring the security table 201, after being generated by the storage controller 40, to the host computers, and making decision of whether they have access right from the table before the hosts themselves issue PLOGI and Inquiry. In this case, the host computers select only the access right portion of themselves from the security table sent from each storage controller and store it. Similarly, a security table may be provided

within the switch or SAN manager provided between the host computer and the storage controller. Thus, the number of commands to be transferred to the fiber channel and commands that the storage controller handles can be decreased, and the I/O process can be more effectively performed.

[0081] Moreover, data damage due to the access from a different protocol, different file system or different OS usually occurs only at the time of data writing. If data reading is controlled to execute from the host computer that has other protocols and different file system, it will be often advantageous. Therefore, it is possible that, as at steps 507 and 508 in Fig. 5, when the user is allowed to enter access right, read access and write access are separately set up so as to provide storage regions allowed only to be read or provide access right only for writing and free access for reading.

[0082] The same vendor sometimes manufactures host computers that have a plurality of different file types. In that case, use of Company_ID might fail to achieve the original security. At that time, a code for identifying OS or file type is added to Company_ID, and this Company_ID can be used to substitute for the Company_ID described in the previous embodiments.

[0083] It is also possible to detect the protocol, file type and OS of host from PLOGI not using N_Port_Name for identifying the host computers, and to use these identification information for Company_ID, so that the same access right can be provided to the host computers of the same file type.

[0084] While a single storage controller and two LUs are used in the above embodiments for the sake of simple explanation, the present invention can be applied to a system having a plurality of storage controllers, or three or more LUs. In this case, the security setting can be of course simplified.

Moreover, the storage region may be logical volume unit, RAID group unit, or physical region or physical volume unit that is not a logically divided unit, other than LU unit. In addition, as in the case where there are provided a plurality of storage units and a plurality of storage controllers, but logically one storage unit and one storage controller, multiple host computers, storage controllers and storage units include the meaning of being both logically multiple and physically multiple ones.

[0085] Furthermore, the recording media may be optical disks or magnetooptical disks other than magnetic disks, or magnetic tape other than disks. The technical field to be applied is not limited to the relation between the host computer and storage controller, but to the relation between other information processors that are required to provide access limitation.

Claims

1. A storage system comprising:

   a storage unit (50) having storage regions for storing data; and
   a storage controller (40) having a back end control unit (46) for controlling the transfer of data from or to said storage unit, a cache (45) for temporarily storing information read from said storage unit, a front end control unit (41) for controlling the transfer of data between said cache and a host computer (10, 20, 30) and a processor (42) that acquires information for identifying said host computer from a frame sent from said host computer and that forces a memory (43) to store said information.

2. A storage system comprising:

   a storage unit (50) having storage regions for storing data; and
   a storage controller (40) having means (42) for identifying storage regions of said storage unit, means (42) for separating information for identifying a host computer (10, 20, 30) from a frame included in a login request from said host computer, a monitor (471) for displaying said connected host computer and said storage regions on the basis of said separated information, a panel (47) for designating a storage region that can be accessed by said host computer with reference to said monitor, and means (42) for setting access right of said host computer to said storage regions on the basis of designation entered through said panel.

3. A storage system according to claim 1 or 2, wherein said information for identifying said host computer is N_Port_Name or World Wide Name.

4. A storage system according to claim 1 or 2, wherein said information for identifying said host computer is Company_ID.

5. A storage system according to claim 4, wherein information of vendor corresponding to said Company_ID is previously stored.

6. A storage system according to claim 1 or 2, wherein information for identifying said host computer (10, 20, 30) is any one of protocol, file type or OS of said host computer.

7. A storage system according to any one of claims 1 through 6, wherein said storage controller is connected to said host computer (10, 20, 30) through a network.

8. A storage system according to any one of claims 1 through 6, wherein said storage controller (40) is connected to said plurality of host computers having

a different protocol and/or a different file system.

9. A storage controller (40) comprising:

a back end control unit (46) for controlling the transfer of data from or to a storage unit (50) under command of said storage controller;
a cache (45) for temporarily storing information read from said storage unit;
a front end control unit (41) for controlling the transfer of data between said cache and a host computer (10, 20, 30); and
a processor (42) for acquiring information for identifying said host computer from a frame sent from said host computer and controlling a memory (43) to store said information.

10. A storage controller (40) comprising:

means (42) for identifying storage regions under command of said storage controller;
means (42) for separating information for identifying a host computer (10, 20, 30) from a frame included in a login request that said host computer issues;
a monitor (471) for displaying said connected host computer and said storage regions on the basis of said separated information;
a panel (472) for designating a storage region that can be accessed by said host computer with reference to said displayed information; and
means (42) for setting the access right of said host computer to said storage regions on the basis of designation entered through said panel.

11. In a storage system having a storage controller (40) and a plurality of host computers (10, 20, 30) connected via a network, a method of setting security for said storage system by said storage controller, comprising:

a step (502) of receiving a frame (70) including information for identifying said host computers (10, 20, 30);
a step (503) of separating said information from said frame and storing said information;
a step (506) of identifying storage regions under command of said storage controller;
a step (507, 510) of generating a table (200, 201, 202; 700) of said host computers and said storage regions on the basis of said separated information; and
a step (508, 511) of designating on said table a storage region that can be accessed by said host computers.

12. In a storage system having a storage controller and a plurality of host computers (10, 20, 30) connected via a network, a method of setting security for said storage system by said storage controller, comprising:

a step (503) of receiving a login request;
a step (503) of separating information for identifying said host computers (10, 20, 30) from a frame (70) included in said login request;
a step (506) of identifying storage regions (50) under command of said storage controller;
a step (507, 510) of displaying said connected host computers and said storage regions on the basis of said separated information;
a step (508, 511) of designating a storage region that can be accessed by said host computers with reference to said displayed information; and
a step (513) of setting the access right of said host computers to said storage regions on the basis of the designation in said designating step.

13. A security setting method according to claim 12, wherein said information for identifying the host computers is any one of N_Port_Name, World Wide Name and Company_ID.

14. In a storage system having a storage controller and a plurality of host computers connected via a network, a method of setting security for said storage system by said storage controller, comprising:

a step (502) of receiving PLOGI;
a step (503) of separating N_Port_Name or World Wide Name from a frame (70) included in said PLOGI;
a step (504) of generating a table associated with said N_Port_Name or World Wide Name and S_ID included in said PLOGI;
a step (503') of deciding if said N_Port_Name or World Wide Name is previously stored;
a step (506) of identifying storage regions under command of said storage controller if said decision is that it is not previously stored;
a step (507, 510) of displaying said connected host computers and said storage regions on the basis of said separated N_Port_Name or World Wide Name;
a step (508, 511) of designating a storage region that can be accessed by said host computers with reference to said displayed information;
a step (513) of setting the access right of said host computers to said storage regions on the basis of the designation in said designating step; and

a step (514) of ordering said host computers to again send PLOGI.

15. A security setting method according to any one of claims 11 through 14, wherein said designation for said accessible storage regions is performed for each of the accesses using separate read command and write command.

16. In a storage system having a storage controller and a plurality of host computers connected via a network, a method of setting security for said storage system by said storage controller,. comprising:

a step (502) of receiving a login request;
a step (503) of separating World Wide Name from a frame (70) included in said login request;
a step (509) of further separating Company_ID from said World Wide Name; and
a step (512) of, when the access right of the same Company_ID to storage regions is already registered, making said access right be used as access right of said host computers that have sent said login request.

17. A security setting method according to any one of claims 11 through 16, further comprising a step of transferring said access right to said host computers.

18. A security setting method according to claim 14, further comprising the steps of, when said host computer (30) is added to said storage system, requesting N_Port_Name or Wold Wide Name to said added host computer in response to a notification (RSCN) that informs of state change of said storage system, adding information of said added host computer to said table and enabling the access right of said added host computer to be set on the basis of said N_Port_Name or World Wide Name from said added host computer.

19. A security setting method according to claim 14, wherein when one (10, 20 or 30) of said host computers is temporarily disconnected from said storage system, information of said disconnected host computer is not changed on said table.

FIG.1

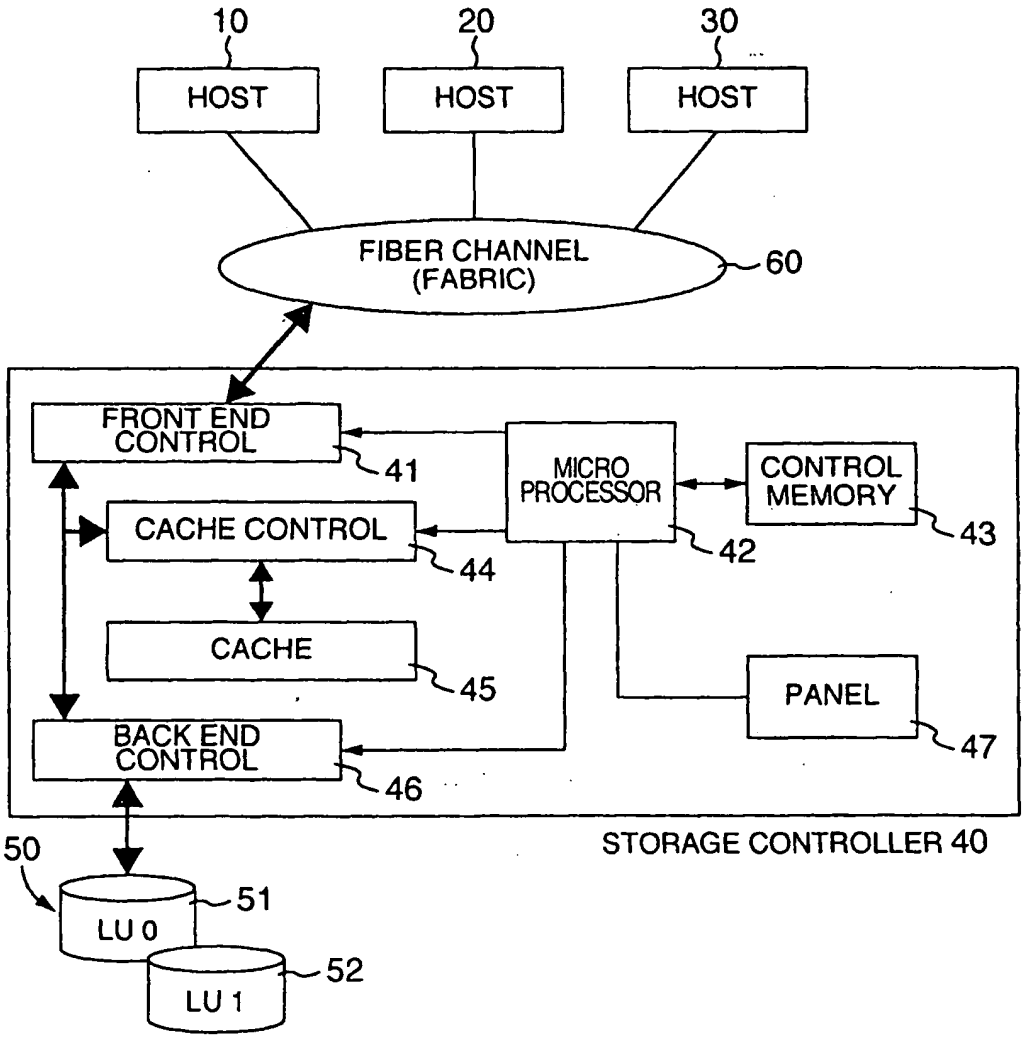

10
20
30
HOST
HOST
HOST
FIBER CHANNEL
(FABRIC)
60
FRONT END
CONTROL
41
MICRO
PROCESSOR
CONTROL
MEMORY
43
CACHE CONTROL
44
42
CACHE
45
PANEL
47
BACK END
CONTROL
46
STORAGE CONTROLLER 40
50
51
LU 0
52
LU 1

FIG.2

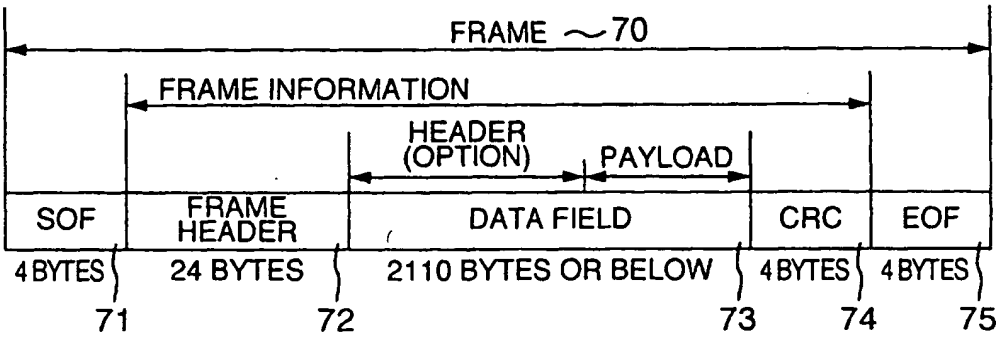


FIG.3

FRAME HEADER ~72

BIT / WORD	31-24	23-16	15-8	7-0
0	R_CTL	D_ID (N_PORT ADDRESS ID ON RECEIVER SIDE)		~81
1	RESERVED	S_ID (N_PORT ADDRESS ID ON TRANSMITTER SIDE)		~82
2	TYPE	F_CTL		
3	SEQ_ID	DF_CTL	SEQ_CNT	
4	OX_ID		RX_ID	
5	PARAMETER			

FIG.4

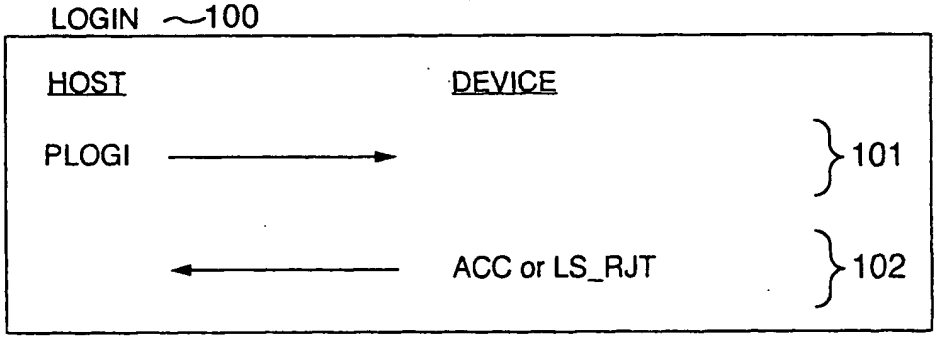


FIG.5

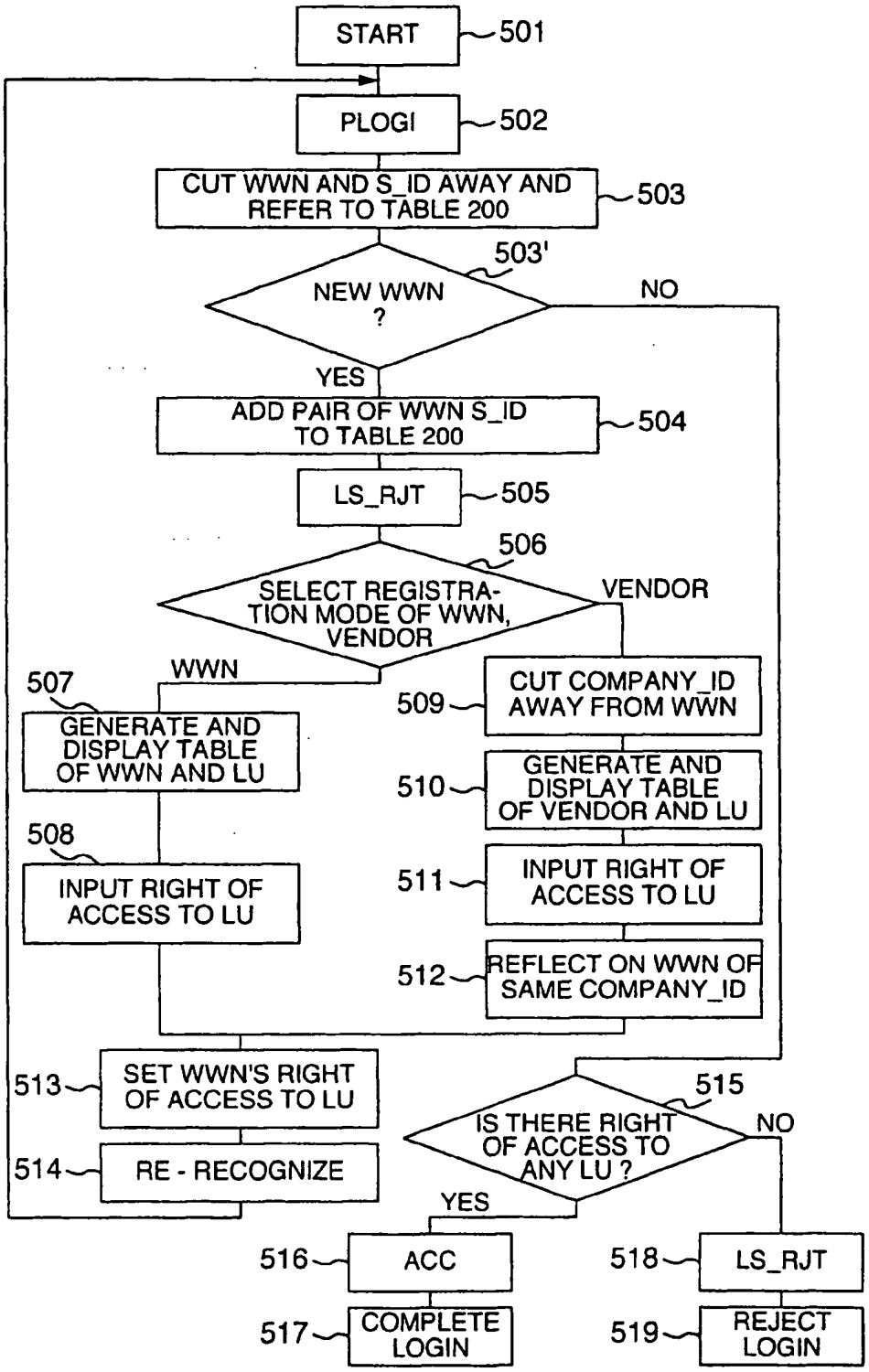

START
501
PLOGI
502
CUT WWN AND S_ID AWAY AND REFER TO TABLE 200
503
503'
NEW WWN ?
NO
YES
ADD PAIR OF WWN S_ID TO TABLE 200
504
LS_RJT
505
506
SELECT REGISTRATION MODE OF WWN, VENDOR
VENDOR
WWN
507
GENERATE AND DISPLAY TABLE OF WWN AND LU
508
INPUT RIGHT OF ACCESS TO LU
509
CUT COMPANY_ID AWAY FROM WWN
510
GENERATE AND DISPLAY TABLE OF VENDOR AND LU
511
INPUT RIGHT OF ACCESS TO LU
512
REFLECT ON WWN OF SAME COMPANY_ID
513
SET WWN'S RIGHT OF ACCESS TO LU
514
RE - RECOGNIZE
515
IS THERE RIGHT OF ACCESS TO ANY LU ?
NO
YES
516
ACC
517
COMPLETE LOGIN
518
LS_RJT
519
REJECT LOGIN

FIG.6

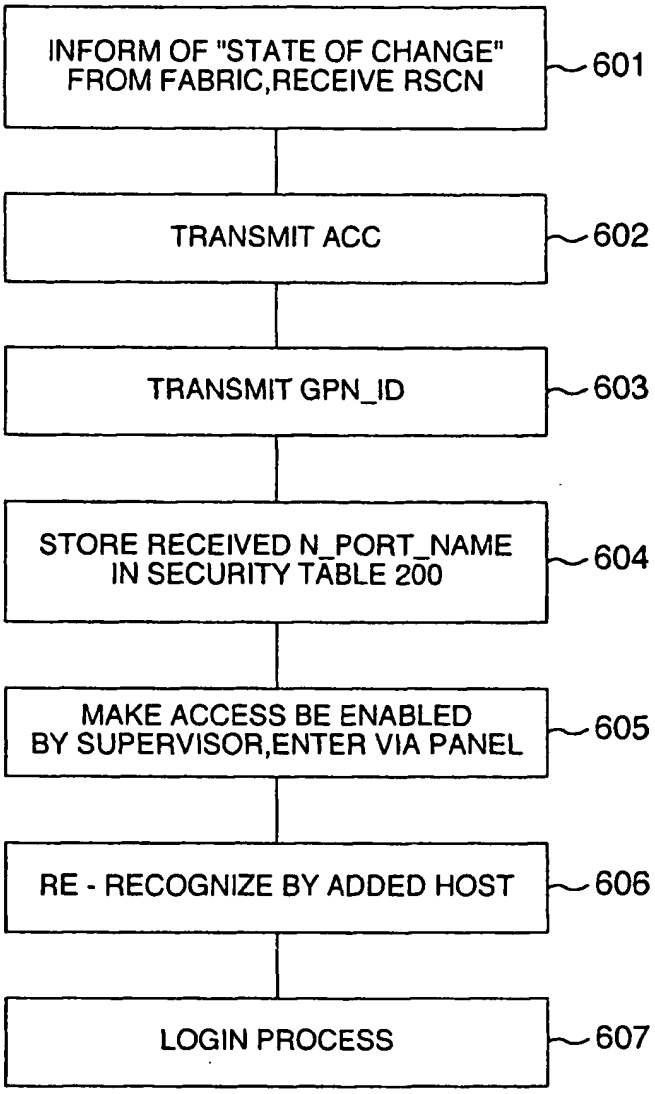

INFORM OF "STATE OF CHANGE" FROM FABRIC,RECEIVE RSCN
601
TRANSMIT ACC
602
TRANSMIT GPN_ID
603
STORE RECEIVED N_PORT_NAME IN SECURITY TABLE 200
604
MAKE ACCESS BE ENABLED BY SUPERVISOR,ENTER VIA PANEL
605
RE - RECOGNIZE BY ADDED HOST
606
LOGIN PROCESS
607

FIG.7A

	WWN	S_ID
HOST A	01234567 89ABCDEF	FFFF01
HOST B	01234567 89ABCDEE	FFFF02
HOST C	01234567 89ABCDED	FFFF03

200

FIG.7B

	ACCESS PERMIT / DENY	
	LU 0	LU 1
HOST A	ENABLE	DISABLE
HOST B	DISABLE	ENABLE
HOST C	DISABLE	ENABLE

201

FIG.7C

	ACCESS PERMIT / DENY	
	LU 0	LU 1
VENDOR A	DISABLE	ENABLE
VENDOR B	ENABLE	DISABLE

202

FIG.7D

WWN	S_ID	ACCESS PERMIT / DENY	
		LU 0	LU 1
01234567 89ABCDEF	FFFF01	ENABLE	DISABLE
01234567 89ABCDEE	FFFF02	DISABLE	ENABLE
01234567 89ABCDED	FFFF03	DISABLE	ENABLE

700

FIG.8

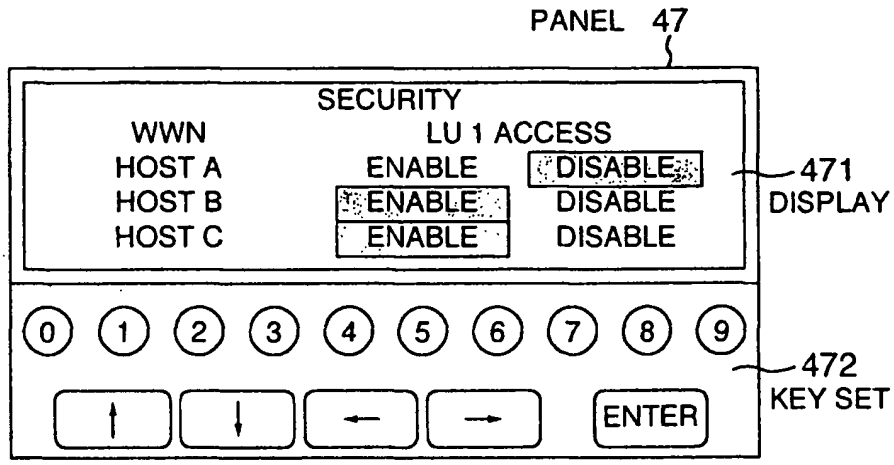

PANEL 47
SECURITY
WWN
LU 1 ACCESS
HOST A
ENABLE
DISABLE
HOST B
ENABLE
DISABLE
HOST C
ENABLE
DISABLE
471
DISPLAY
0
1
2
3
4
5
6
7
8
9
ENTER
472
KEY SET

FIG.9

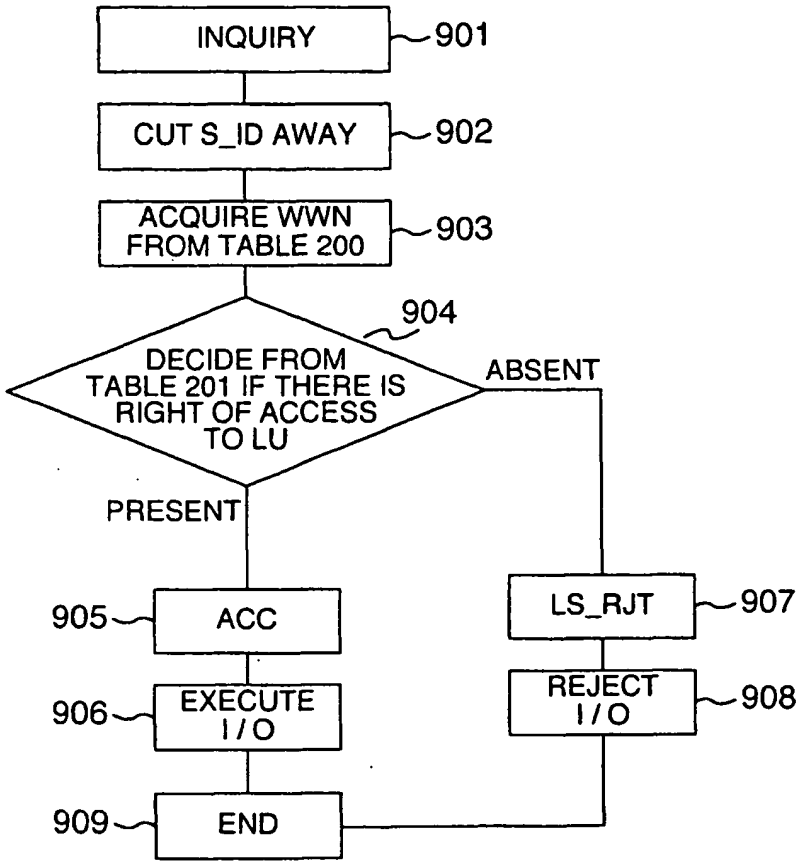

INQUIRY
901
CUT S_ID AWAY
902
ACQUIRE WWN FROM TABLE 200
903
904
DECIDE FROM TABLE 201 IF THERE IS RIGHT OF ACCESS TO LU
ABSENT
PRESENT
905
ACC
907
LS_RJT
906
EXECUTE I/O
REJECT I/O
908
909
END

FIG.10

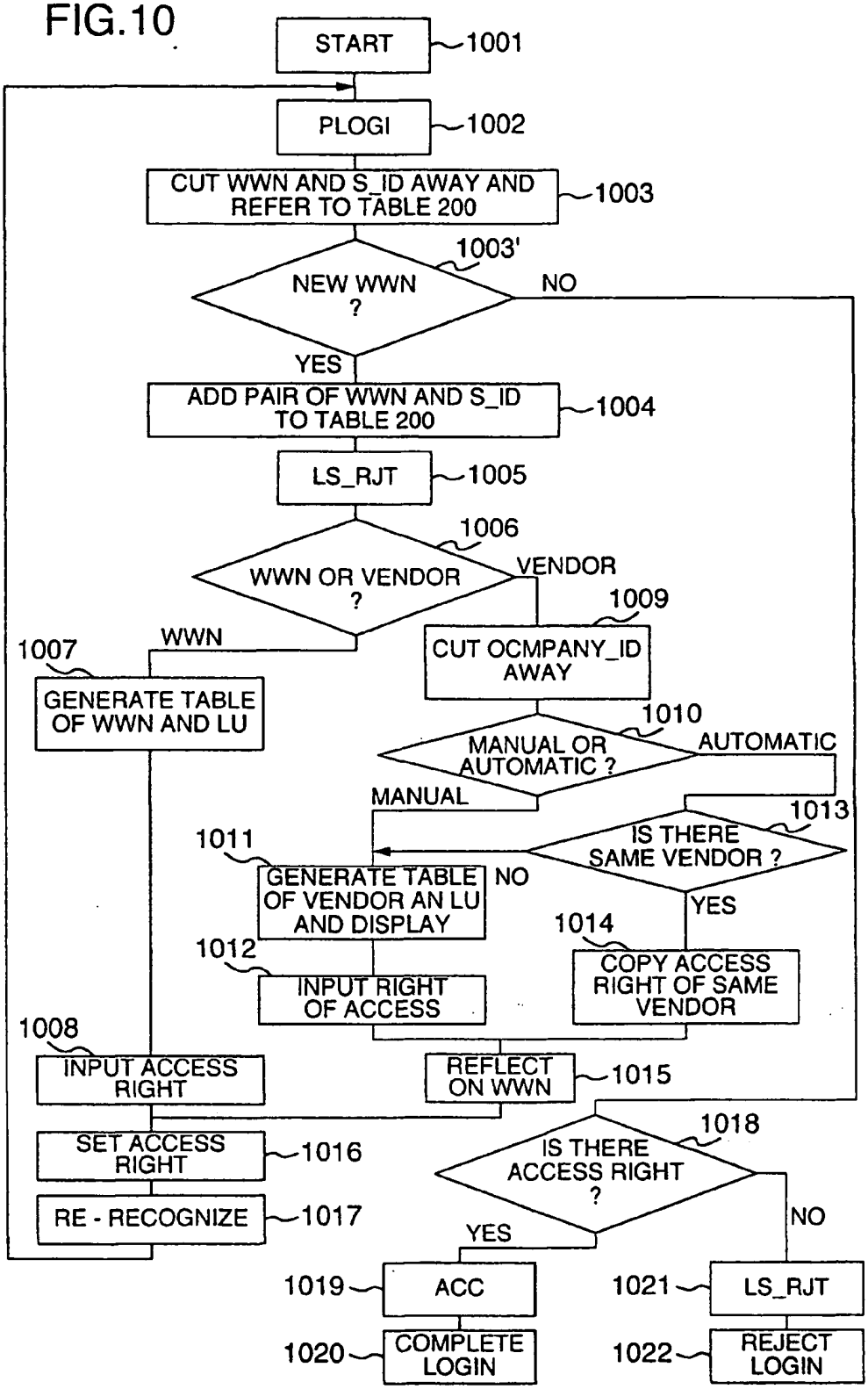

START
1001
PLOGI
1002
CUT WWN AND S_ID AWAY AND REFER TO TABLE 200
1003
1003'
NEW WWN ?
NO
YES
ADD PAIR OF WWN AND S_ID TO TABLE 200
1004
LS_RJT
1005
1006
WWN OR VENDOR ?
VENDOR
1009
WWN
1007
CUT OCMPANY_ID AWAY
GENERATE TABLE OF WWN AND LU
1010
MANUAL OR AUTOMATIC ?
AUTOMATIC
MANUAL
1013
1011
IS THERE SAME VENDOR ?
GENERATE TABLE OF VENDOR AN LU AND DISPLAY
NO
YES
1014
1012
COPY ACCESS RIGHT OF SAME VENDOR
INPUT RIGHT OF ACCESS
1008
INPUT ACCESS RIGHT
REFLECT ON WWN
1015
1018
SET ACCESS RIGHT
1016
IS THERE ACCESS RIGHT ?
RE - RECOGNIZE
1017
NO
YES
1019
ACC
1021
LS_RJT
1020
COMPLETE LOGIN
1022
REJECT LOGIN

FIG.11

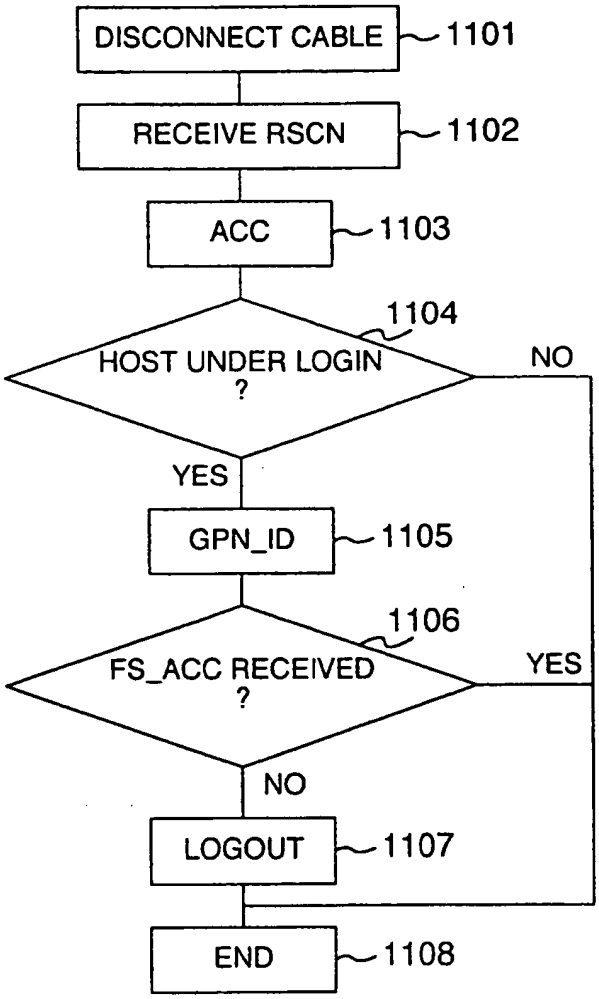

DISCONNECT CABLE
1101
RECEIVE RSCN
1102
ACC
1103
1104
HOST UNDER LOGIN ?
NO
YES
GPN_ID
1105
1106
FS_ACC RECEIVED ?
YES
NO
LOGOUT
1107
END
1108

FIG.12

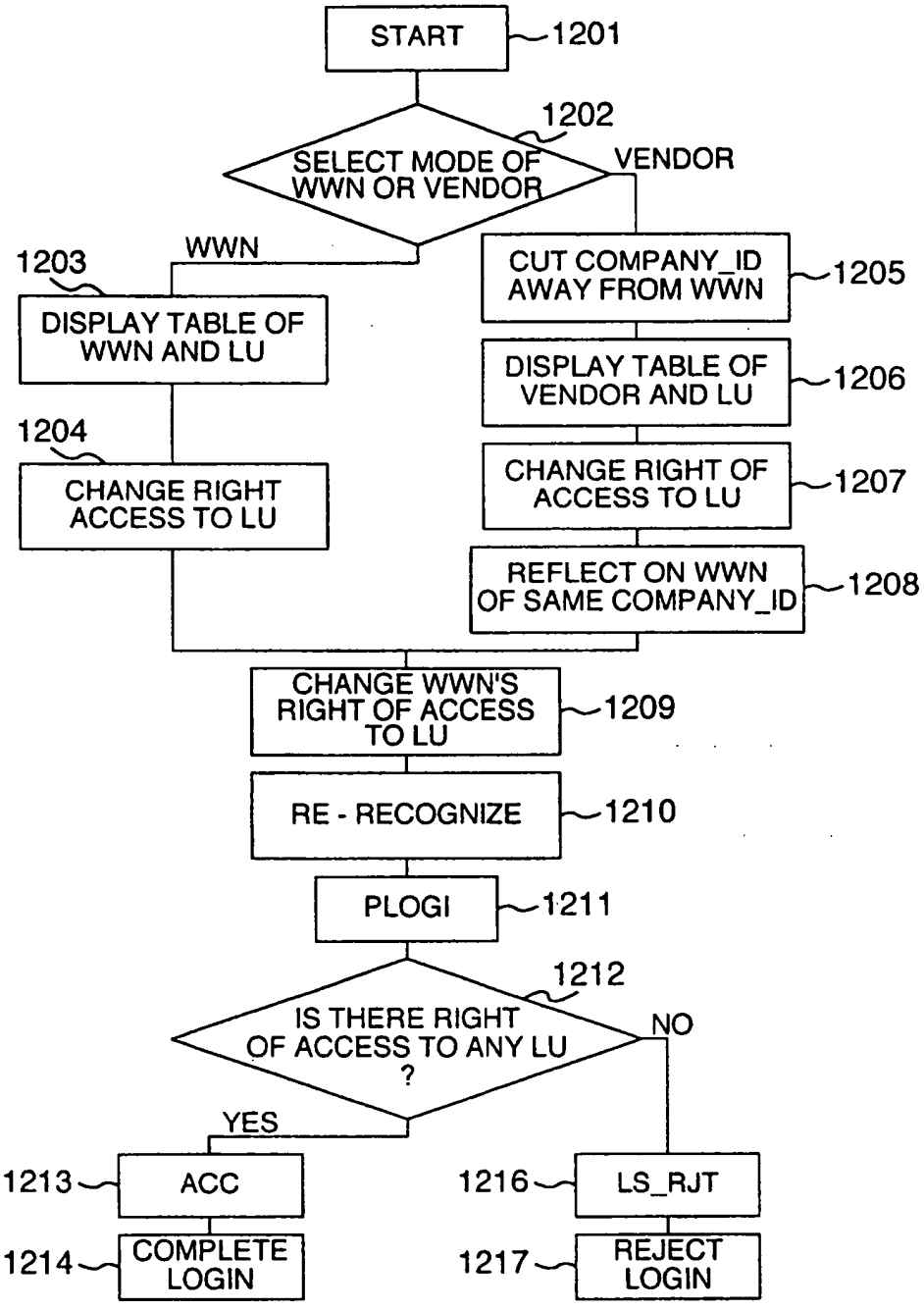
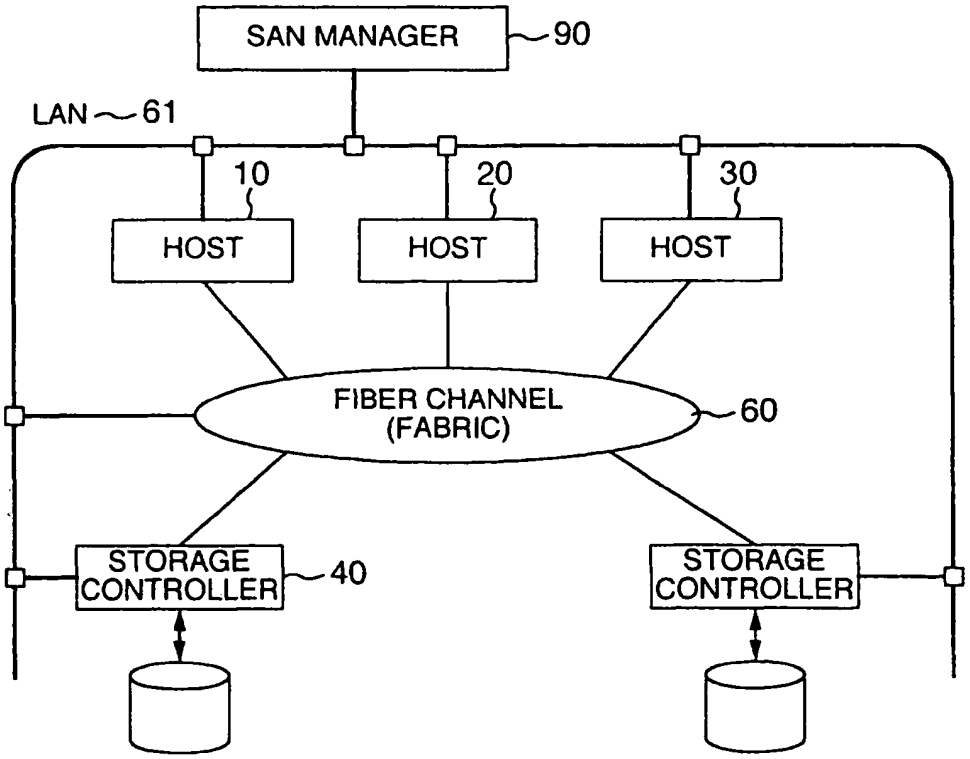

START
1201
1202
SELECT MODE OF WWN OR VENDOR
WWN
VENDOR
1203
DISPLAY TABLE OF WWN AND LU
1204
CHANGE RIGHT ACCESS TO LU
CUT COMPANY_ID AWAY FROM WWN
1205
DISPLAY TABLE OF VENDOR AND LU
1206
CHANGE RIGHT OF ACCESS TO LU
1207
REFLECT ON WWN OF SAME COMPANY_ID
1208
CHANGE WWN'S RIGHT OF ACCESS TO LU
1209
RE - RECOGNIZE
1210
PLOGI
1211
1212
IS THERE RIGHT OF ACCESS TO ANY LU ?
NO
YES
1213
ACC
1214
COMPLETE LOGIN
1216
LS_RJT
1217
REJECT LOGIN

FIG.13


SAN MANAGER
90
LAN
61
10
20
30
HOST
HOST
HOST
FIBER CHANNEL
(FABRIC)
60
STORAGE
CONTROLLER
40
STORAGE
CONTROLLER